SC402- Introduction to Cryptography
Assignment 1

1. Use exhaustive key search to decrypt the following ciphertext, which was encrypted using a *Shift Cipher*:

   `BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKFUHCQD.`

2. Determine the number of keys in an Affine Cipher over $\mathbb{Z}_m$ for $m = 30, 100$ and 1225.

3. List all the invertible elements in $\mathbb{Z}_m$ for $m = 28, 33$ and 35.

4. (a) Suppose that π is the following permutation of $\{1, \ldots, 8\}$:

x	1	2	3	4	5	6	7	8
$\pi(x)$	4	1	6	2	7	3	8	5

   Compute the permutation π^{-1} .

   (b) Decrypt the following ciphertext, for a Permutation Cipher with $m = 8$, which was encrypted using the key π:

   `TGEEMNELNNTDROEOAAHDOETCSHAEIRLM.`

5. Suppose we are told that the plaintext

   `breathtaking`

   yields the ciphertext

   `RUPOTENTOIFV`

   where the Hill Cipher is used (but m is not specified). Determine the encryption matrix.

6. An *Affine-Hill Cipher* is the following modification of a *Hill Cipher*: Let m be a positive integer, and define $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$. In this cryptosystem, a key K consists of a pair (L, b), where L is an $m \times m$ invertible matrix over $\mathbb{Z}_{26}$, and $b \in (\mathbb{Z}_{26})^m$. For $x = (x_1, \ldots, x_m) \in \mathcal{P}$ and $K = (L, b) \in \mathcal{K}$, we compute $y = e_K(x) = (y_1, \ldots, y_m)$ by means of the formula $y = xL + b$. Hence, if $L = (\ell_{i,j})$ and $b = (b_1, \ldots, b_m)$, then

$$(y_1, \ldots, y_m) = (x_1, \ldots, x_m) \begin{pmatrix} \ell_{1,1} & \ell_{1,2} & \ldots & \ell_{1,m} \\ \ell_{2,1} & \ell_{2,2} & \ldots & \ell_{2,m} \\ . & . & \ldots & . \\ . & . & \ldots & . \\ . & . & \ldots & . \\ \ell_{m,1} & \ell_{m,2} & \ldots & \ell_{m,m} \end{pmatrix} + (b_1, \ldots, b_m).$$

   Suppose Oscar has learned that the plaintext

   `adisplayedequation`

   is encrypted to give the ciphertext

   `DSRMSIOPLXLJBZULLM`

   and Oscar also knows that $m = 3$. Determine the key, showing all computations.

7. Decrypt the following ciphertext, obtained from the *Autokey Cipher*, by using exhaustive key search:

   `MALVVMAFBHBUQPTSOXALTGVWWRG.`